ELECTRONIC TRANSACTION SECURITY METHOD

FIELD OF THE INVENTION

The present invention relates to the electronic processing of credit card transactions.

BACKGROUND OF THE INVENTION

Credit cards are commonly used over the public Internet to purchase goods and services. The information required to initiate a transaction consists of a credit card number, an expiration date for the card, a cardholder's billing address and the card holder's name as shown on the card. All of the information made available to support a credit card transaction may become known to a third party who is then in a position to use the same without the consent or knowledge of the cardholder. The fact that the credit card information can be re-used by a third party without the consent or knowledge of the card holder creates a problem for both the cardholder and the institution that issued the credit card.

SUMMARY OF THE INVENTION

A primary object of this invention is to provide a method and arrangement for securing electronic transactions against fraud.

Another object of this invention is to provide a method and an arrangement that serves to limit the useful lifetime of credit card transaction information.

A more specific object of the present invention is to define a method and an arrangement that creates or enables, at the time that an electronic credit card transaction is initiated, a date/time stamp that is based on or obtained from a non-adjustable clock. The date/time stamp is embedded in or accompanies the

credit card transaction information provided by the user and serves to limit the useful lifetime of that transaction information. The method and arrangement also provides for checking the date/time stamp against a non-adjustable clock the instant that the credit card transaction information is received to verify that the transaction information is valid and that the transaction should proceed. The method of the present invention is applicable to all credit card transactions as well as other electronic transactions that need or would benefit from a limit on the useful lifetime of transaction information.

With respect to the method of the present invention, it is to be understood that a non-adjustable clock is an accurate clock which is fixed in the sense that it cannot be adjusted by a party to the electronic transaction and which is available to both the initiator and validator of the transaction. It is contemplated the initiator and the validator may access different non-adjustable clocks provided that they provide identical internet times (net-time). A net-time date/time stamp is understood to be a date/time stamp created from a non-adjustable clock available on the internet. To allow for different time zones at the locations of the initiator and validator, the date/time stamp is keyed to a common time standard, e.g., Greenwich mean time. The most common on-line sources for a non-adjustable clock are accessible on servers run by the U.S. government and other institutions. A preferred source is the master clock of the U.S. Naval Observatory. The latter is available on line on the internet at the following address: http://tycho.usno.navy.mil". The method of the present invention allows for the use of any encryption scheme whereby the encryption technique is supplied by the credit card institution or provider of the method.

BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention is depicted in the drawings and elucidated in the following description, in which:

Fig. 1 shows a software flowchart representing the method of the present invention.

Fig. 2 shows a software flowchart of an alternative embodiment of the method of the present invention.

DETAILED DESCRIPTION

A typical credit card transaction consists of an account number, a credit card holder's name and a credit card expiration date. Occasionally other information, e.g., a personal identification number (PIN), may be gathered to help validate the transaction (the PIN, which may be represented by a sequence of alphanumeric characters in any combination, is intended to be known only to the issuing institution and the customer or user). All of this credit card information is passed to the entity that is brokering the transaction, namely the credit card issuer or another party acting on behalf of or for the credit card issuer, for verification and validation . In the usual case the information is transmitted to the validating institution by a third party vendor. However, it is understood that in some cases the user may deal directly with the validating institution, e.g., where the credit card issuer is a bank with whom the user has a bank account and the user desires to execute an electronic transfer of funds from his bank account. The present invention improves on the security of electronic financial transactions by including an encrypted date/time stamp that is passed along as part of the information required to secure the transaction against fraud, i.e., to obtain validation of the transaction information. The encryption scheme may use all or part of a credit card account number and/or a PIN known only to the cardholder and the institution issuing the credit card to ensure that the date/time stamp cannot be generated by an unauthorized entity.

The software that implements the method of this invention may be embedded in the user's (customer's) web browser or may be a separate program that can be accessed on command by that web browser. The software maybe in

the form of an active X-control, a Java applet, or any other program that can execute in a web browser.

According to a preferred embodiment of the invention, the software that executes in the browser first obtains a date/time stamp from a known non-adjustable time source such as the master clock of the U.S. Naval Observatory, and then encrypts it using a predetermined encryption technique or program. The encrypted date/time stamp is passed along with other credit card transaction information to a validating institution for processing, as described hereinafter. In this preferred embodiment, an example code fragment of the embedded software code is:

```
x = nettime( );
y = encrypt(x);
return y;
```

where "nettime" is the date/time data obtained from a non-adjustable time source.

Further details of the preferred embodiment of the present invention are presented in the following description of the method illustrated by Fig. 1. This method assumes as a preliminary matter that individual credit card accounts have been established by a credit card issuer for a number of different users and that each account and its authorized user (credit card holder or a person authorized to act for the card holder) are identified by one or more unique identification codes, and also that the account and user identification codes and other information pertaining to each account is stored in a data base created and maintained by the credit card issuer and/or some other party authorized by the credit card issuer to validate proposed credit card transactions on behalf of the credit card issuer. It is to be understood also that the method of Fig. 1 applies to electronic transactions involving only the credit card user and the credit card issuer or validating institution, as well as to transactions involving a third party vendor from whom the user wishes to purchase goods or services. Accordingly,

although not shown in Fig. 1, it is to be understood that if the proposed transaction involves a third party vendor, the transmittal of information between the user and validating institution is conducted via the vendor's server. With the foregoing in mind, Fig. 1 comprises the following steps:

1. Using an internet browser, the consumer or customer (user) executes a software application according to the invention for the purpose of initiating a credit card transaction. The software is designed to carry out the method represented in Fig. 1 and includes a component supplied by the credit card processing institution (and embedded in the software application or the browser) which is adapted to obtain and encrypt a date/time stamp, delivering an encrypted date/time stamp in the form of a series of alphanumeric values.

2. The transaction is initiated by filling out a transaction information form that is made available by the software application through an internet browser. Such a form is commonly used by on-line retailers for the collection of personal information including the name, address, and credit card number of the consumer, and the credit card expiration date..

3. After the credit card transaction information is gathered, a date/time stamp is obtained from a non-adjustable time source via the internet.

4 The date/time stamp is encrypted by the software program executed in the browser for inclusion with the credit card information to be transmitted. Various encryption programs known to persons skilled in the art may be used for this invention since the type of encryption technique is not critical to the invention described here. However, it is to appreciated that the better the encryption technique, the more secure the transaction will be. What is important is that the selected encryption scheme be known only to the institution validating the transaction and to the software that encrypts the date /time stamp when the customer information is entered.

5. The encrypted date/time stamp and the other information representing the proposed transaction (the "document") is transmitted via the

internet to a destination where it is to be validated. In the case where the transaction is being conducted with a third party vendor via the internet, transmission of the transaction information to the validating institution is accomplished via the vendor's server. Preferably this is done automatically by the vendor's server; alternatively it may be done only on command by the vendor.

6. On arrival at the validating institution's server, the credit card holder's transaction information is compared with credit card information stored in or available to that server in order to verify that the transaction is initiated by an authorized user, as is normal practice for existing credit card transaction systems. In this case, the verification and validation process involves decrypting the date/time stamp using the selected decryption technique to determine the exact time that the transaction was initiated.

7. The decrypted date/time stamp representing the exact time the truncation was initiated is compared with a new date/time stamp created from the time obtained by the validating institution from a non-adjustable time source via the internet. The difference between (a) the time of the date/time stamp assigned to the transaction (the "transaction date/time stamp") and (b) the new date/time stamp representing the time obtained by the validating institution from the non-adjustable time source is then compared with a known time limit known only to the entity that has the responsibility of validating or rejecting the transaction. If the time limit has been exceeded the transaction is considered not to be valid and is rejected, and the rejection is communicated back to the vendor and/or the car holder or other party who initiated the transaction. If the time difference is at or within the time limit, the transaction is validated (provided, of course, that the remainder of the transaction information has been deemed valid) and that transaction validation is communicated back to the vendor and card holder or other party who initiated the transaction process.

Fig. 2 illustrates another embodiment of the invention for use when a credit card issuer wishes to use a PIN (personal identifier number) and a public/private key encryption technique to secure the transaction. The validating institution, e.g., the credit card issuer, selects the encryption technology to be used. As with the embodiment of Fig. 1, various encryption programs known to persons skilled in the art may be used for this invention since the type of encryption technique is not critical to the invention described here. However, it is to appreciated that the better the encryption technique, the more secure the transaction will be. What is important is that the encryption scheme be known only to the institution validating the transaction and to the software that encrypts the date /time stamp when the customer information is entered. An advantage of a number of known public/private key encryption methods that may be used for this invention is that they are easy to use while providing transaction privacy.

As with the method of Fig. 1, this embodiment assumes as a preliminary matter that (a) individual credit card accounts have been established by a credit card issuer for a number of different users and that each account and its authorized user(s) are identified by unique identification codes, (b) a PIN has been assigned to each authorized user which is known only to the credit card issuer, the validating institution (if different from the credit card issuer), and the credit card holder or a user authorized by the credit card holder. It is to be understood also that the method of Fig. 2 applies to electronic transactions involving only the credit card user and the credit card issuer or validating institution, as well as to transactions involving a third party vendor from whom the user wishes to purchase goods or services. Accordingly, although not shown in Fig. 2, it is to be understood that if the proposed transaction involves a third party vendor, the transmittal of information between the user and validating institution is conducted via the vendor's server

Referring now to Fig. 2, the method illustrated therein comprises the following steps

1. Using an internet browser, the consumer or customer executes a software application embodying the invention for the purpose of initiating a credit card transaction. As with the preferred embodiment of the invention represented in Fig. 1, the software application includes a component supplied by the credit card processing institution (and embedded in the software application or the browser) which is adapted to obtain and encrypt a date/time stamp, delivering an encrypted date/time stamp in the form of a series of alphanumeric values

2. The customer or user records (a) personal information required by the vendor for the transaction, e.g., name and address of the customer or other user, (b) a public key number (PKN), and (c) a private key number (the PIN). An example of a PKN is a credit card account number. However, the credit card issuer or other validating institution may elect to require use of another alphanumeric sequence as the PKN in addition to or in place of the credit card account number. As an alternative approach, it is envisioned that the public key (PKN) may be the PIN and the private key may be something known only to the institution and the ePIN software generator.

3. A date/time stamp is obtained from a non-adjustable time source via the internet, as described above.

4. The PIN and the date/time stamp are converted to an ePIN for transmission via the internet. In this step the software program uses the PIN along with the date/time stamp as the basis for creating an encrypted sequence of alphanumeric characters that constitute the ePIN. The latter hides the PIN and the date/time stamp so that they can be retrieved only by the validating institution. As an alternative approach, the software program may be designed to use all or part of the PKN as well as the PIN and the date/time stamp to generate the ePIN.

5. The data representing the transaction (the "document") is transmitted via the internet to the validating institution. The document includes the ePIN and the PKN, as well as other transaction data entered by the user

which is requested by the validator, e.g., name and account number of the credit card holder. If a third party vendor is involved in the proposed transaction, the transmission of the data to the validating institution is accomplished via the vendor's server, and this may be done automatically or on command by the vendor.

6. The validating institution decrypts the ePIN to obtain the PIN and the date/time stamp.

7. The validating institution looks up the user's PIN in its database to determine if the transmitted PIN is valid. If it is valid, the checking continues; otherwise the transaction is rejected, and the rejection is communicated to the vendor and/or the customer or other party who initiated the transaction.

8. Next the validating institution checks the age of the transaction. More specifically, the decrypted date/time stamp representing the exact time the transaction was initiated is compared with a new date/time stamp created from the time obtained by the validating institution from a non-adjustable time source via the internet. The difference between the time of the date/time stamp assigned to the transaction (the "transaction date/time stamp") and the new date/time stamp representing the time obtained by the validating institution from the non-adjustable time source is compared against a known time limit known only to the entity that has the responsibility of validating or rejecting the transaction. If the time limit has been exceeded, the transaction is considered not to be valid and is rejected. If the time limit has not been exceeded, the transaction is validated (provided, of course, that the remainder of the transaction has been verified as being correct). As in step 7, the rejection is communicated to the vendor and/or the customer or other party who initiated the transaction.

With respect to validating the date/time stamp, it is to be understood that the credit card issuer or other validating institution sets the time period for a transaction to be valid, and that its server may be programmed to validate not

only transactions which are presented for validation within the time limit but also those which exceed the time limit by a predetermined tolerance magnitude, e.g., to compensate for time delays due to heavy transaction traffic. Also although (a) the time represented by the date/time stamp is the time that the stamp is generated from the non-adjustable time source and (b) the date stamp may not be transmitted to the validating institution instantaneously upon being generated, for convenience it may be deemed to be and is characterized herein as the time that the proposed transaction is initiated, or as the "current transaction time", since the time difference is quite small, generally in the order of seconds.

It is contemplated that the invention may be practiced other than as described above. Thus according to an alternative version of the foregoing embodiments, the software executed in the browser first obtains a date/time stamp from a non-adjustable time source via the internet, but the encrypted date/time stamp is not generated by the program accessed by the user's browser; instead the date stamp is encrypted by the validating institution (validator) and delivered to the user's (initiator's) browser via the internet. Accordingly, in this embodiment, the software code embedded in the browser may comprise the following:

```
y = GetEncrytedDateTimeFromInstitution();
return y;
```

The embedded code for GetEncrytedDateTimeFromInstitution() is:

```
OpenSocket(InstitutionServer);
GetEncryptedDateTimeStamp( );
Close Socket( ):
```

For this embodiment, the Credit Card Institution Server contains the following code fragment:

```
x = nettime();
y = encrypt(x);
return y
```

Other variations of the invention will be obvious to persons skilled in the art

The invention offers several advantages. For one thing, it can be implemented using known programming and encryption techniques. Secondly, it requires no special computer or communication equipment and hence can be implemented at relatively low cost. Thirdly it safeguards electronic transactions against fraud by introducing an additional layer of user identification that is time limited and hence is difficult, if not impossible, to circumvent. Fourthly it may be used to safeguard other electronic transactions in addition to ordinary credit card transactions involving a customer, a vendor and the credit card issuer, e.g., orders to transfer funds from a bank or other credit account. Other advantages will be obvious to persons skilled in the art.